AMAZON CONFIDENTIAL

FMI Consultation
Prudential Policy Department
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140
[by email: fmiconsultation@rbnz.govt.nz]

18 November 2022

Re: Consultation on RBNZ and FMA's FMI Standards exposure drafts

Dear Sir/Madam,

Amazon Web Services (AWS) welcomes the opportunity to comment on the FMI Standards Exposure Drafts (Standards) and Financial Market Infrastructures Standards: Exposure Draft Guidance (Guidance) published by the Reserve Bank of New Zealand (RBNZ) and the Financial Markets Authority (FMA).

Introduction

AWS is the cloud computing arm of Amazon Inc. AWS has been operating in New Zealand since 2013. We have offices in Auckland and Wellington. In September 2021, AWS announced that it would establish an AWS Region in Auckland in 2024, which will bring world-class cloud computing infrastructure onshore to New Zealand. The Economic Impact Study[1] that accompanied the AWS infrastructure announcement estimated that this investment of NZD$7.5 billion will create around 1,000 new jobs and contribute approximately NZD$10.8 billion to New Zealand's GDP over 15 years. AWS allows customers, including many financial services industry customers, to innovate and scale in a highly secure cloud environment. The forthcoming AWS infrastructure in Auckland will enable our thousands of New Zealand customers – from large enterprises to government to small businesses and individuals – to leverage our advanced cloud services using infrastructure located in New Zealand.

AWS Comments

AWS welcomes and is supportive of the RBNZ and FMA's principles-based approach to setting prudential standards. We believe the Standards and Guidance strike a good and workable balance. Our commentary is limited to the sections of the Standards and Guidance relevant to AWS and its customers. These are Standard 17A (Contingency Plans), Standard 17B (Critical Service Providers), Standard 17C (Cyber Resilience) and Standard 23B (Notifying the Regulator).

[1] AWS Economic Impact Study, New Zealand Region

We have outlined areas of concern and we make **ten recommendations** for changes below primarily to the Guidance document. We also attach Appendix A which contains additional issues for consideration by the RBNZ and FMA.

We would welcome the opportunity to discuss our submission. As detailed below, a number of the statements relating to cloud services are, in our view, overly broad and do not sufficiently distinguish between the distinct operating models and capabilities of different cloud service providers. Simply put: not all cloud services are the same. Accordingly, we would be grateful for the opportunity to brief the authors on the capabilities and operating models of hyperscale public cloud technology such as AWS prior to finalisation of the Guidance, particularly in relation to security, resilience and other data protection considerations that are addressed in the Standards and Guidance.

Key issues

Statements on the heightened risk associated with the use of cloud service providers (Guidance 17C.76 to 17C.80)

Although AWS appreciates the positive messaging in Section 17C.76 of the Guidance in relation to the benefits of cloud adoption, AWS is concerned that FMI operators may interpret some statements in Sections 17C.76 and 17C.80 of the Guidance as implying that it is inherently riskier (a) to use cloud services (rather than alternatives such as "on-premises" IT infrastructure), (b) to use a single cloud service provider (rather than a multi-cloud solution), or (c) to store data offshore. This could limit FMI operators' ability to use the most appropriate IT infrastructure and services for their needs. In particular, we are concerned that cloud is described as a source of concentration risk requiring "special attention" and early regulatory notification if an FMI operator intends to outsource essential services to a cloud service provider.

There are several reasons why we consider this Guidance as potentially counterproductive for FMI:

- First, hyper-scale cloud service providers typically have substantially more secure and resilient IT infrastructure than alternatives such as smaller cloud service providers or smaller-scale infrastructure owned and managed by FMI operators themselves. Cloud adoption in fact represents a risk reduction opportunity for the financial services industry as it modernizes and moves away from legacy technology that in some instances is many decades old.
- Second, cloud service providers proactively mitigate potential geographic and concentration risks by offering customers the ability to use services across physically separate locations and logically segregated IT systems. For example, AWS's Cloud infrastructure is built around AWS Regions, which are separate physical locations with multiple Availability Zones. AWS Availability Zones consist of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities that offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data centre. AWS currently has 29 Regions around the world, comprising a total of 93 Availability Zones. The AWS Sydney region has been running since 2012, the AWS Melbourne region will launch shortly, and the AWS Auckland region (using the same multiple Availability Zone model as all other regions) will be launched in 2024.
- Third, many customers have found thatmulti-cloud strategies require them to attempt to standardise on lowest common denominator services between cloud service providers, which may vary significantly in maturity and capability.
- Fourth, even if multiple FMIs exclusively use the same cloud service provider, this would not create a problematic concentration risk so long as that service provider's infrastructure and services are offered via physically separate locations and are designed to be highly secure and resilient. For

example, AWS mitigates this as every customer's workload deployment on AWS is different, which means that no two customers are exposed to the same technology and geography risks.

Recommendation 1: AWS respectfully recommends that the RBNZ and FMA consider removing references in Sections 17C.76 to 17C.80 (Outsourcing to Cloud Service Providers) that appear to imply that using cloud is inherently riskier for FMIs. We would very much welcome the opportunity for further dialogue with the RBNZ and FMA prior finalising the Guidance to address concerns that cloud services provision is inherently riskier than other service delivery models, and to provide additional information regarding the security, resilience and compliance capabilities of a hyperscale public cloud service provider such as AWS. Specifically, we recommend that the RBNZ and FMA **delete** the following in order to address the concerns outlined above:

> **(a)** "However, using cloud services brings challenges to assess legal and regulatory obligations and operators may also run the risk of potentially underinvesting in risk mitigation if the shared tasks are not well articulated and understood. The trend of relying on a narrow set of major cloud service providers also puts concentration risks on the financial system. Therefore, operators should pay special attention when outsourcing to cloud service providers." from Section 17C.76 of the Guidance; and
>
> **(b)** Sections 17C.77(a) and 17C.77(d) of the Guidance.

Management of third-party service providers (Guidance 17C.57 to 17C.58)

AWS welcomes the positive language regarding the benefits of prudently using third party providers to reduce cyber risk. However, AWS is concerned that some comments in Sections 17C.57 and 17C.58 of the Guidance create the impression that using *any* third party service provider will inherently weaken an FMI's cyber resilience and make the FMI an easier target for cyber criminals. We contend strongly that this is not true in all cases particularly for those third parties, such as AWS, which invest in security as their top priority and provide significant resources and expertise to help significantly improve their customers' security and resilience. Additionally, New Zealand as elsewhere, has a range of specialised third party cyber security partners that provide excellent, industry leading services to improve cyber resilience.

Section 17.C.57 of the Guidance states that "the third-party ecosystem provides an environment that makes it easier for cyber criminals to infiltrate an organisation." AWS disagrees with this statement and is concerned that this language will cause operators to avoid outsourcing even when outsourcing could significantly improve their operational and cyber resilience. We recognise that there is a broad spectrum of third-party service providers, however, many third-party service providers can provide operators with services that significantly reduce the risk of cyber-attacks. For example, hyperscale cloud service providers like AWS offer access to significantly more security features, and cyber security countermeasures than almost any large company could afford to provision for themselves. AWS's core infrastructure is built to satisfy the security requirements of military, global banks, and other high-sensitivity organisations, and AWS's service offerings and associated supply chain are vetted and accepted as secure enough for top secret workloads. This is backed by a deep set of cloud security tools, with over 300 security, compliance, and governance services and key features. AWS also provides a wide variety of best practices documents, encryption tools, and other guidance that customers can leverage. In addition, AWS partners offer hundreds of tools and features to help customers meet their security objectives, ranging from network security, configuration management, access control, and data encryption. This security and compliance posture is backed up by numerous certifications and attestations by third party auditors.

Recommendation 2: AWS recommends that the RBNZ and FMA delete "However, the third-party ecosystem provides an environment that makes it easier for cyber criminals to infiltrate an organisation"

from Section 17.C.57 of the Guidance. Alternatively, we suggest that the RBNZ and FMA modify this Section as follows:

> "However, **if operator does not conduct appropriate due diligence on a third-party service provider's control environment and if access to systems and data are improperly configured and managed,** the third-party ecosystem **may** provide an environment that makes it easier for cyber criminals to infiltrate an organisation."

Section 17C.58 of the Guidance states that (a) the extensive use of third party services increases the difficulty of assessing an FMI's level of cyber resilience and exposure to cyber risk, and (b) introduces additional vulnerabilities and threats via third party service providers using other service providers. We consider these statements to be overly broad and not accurate in all cases. For example, hyperscale cloud service providers, like AWS, can provide high levels of transparency and visibility into their operating environments and typically have rigorous compliance programs and certifications that are audited and reported on by independent third parties (e.g. AWS Compliance Programs). We believe AWS makes it significantly easier for FMIs and regulators to assess the level of cyber resilience and exposure to cyber risk as AWS customers may download copies of these reports and certifications from AWS Artifact for free. Further, not all third party service providers rely on other service providers – and those that do, do not necessarily rely on service providers that increase the cyber risk for FMIs. In some cases, third party service providers utilise other service providers to bolster their own cyber resilience and operations.

Recommendation 3: AWS recommends that the RBNZ and FMA delete Section 17C.58 of the Guidance. Alternatively, we recommend amending Section 17C.58 to ensure that these statements do not apply to all third party service providers as follows:

> **"Depending on the nature and maturity of a third-party service provider**, extensive use of third-party services **may** increase the difficulty of assessing an FMI's level of cyber resilience and exposure to cyber risk, both for the FMI itself and its regulators. In addition, third parties **may** ~~increasingly~~ rely on other service providers, **which may** introduce additional vulnerabilities and threats.**"**

Consultation on changes to technology (Guidance 17B.14)

Section 17B.14 of the Guidance requires critical service providers to undertake comprehensive consultation with an operator and, where relevant, its participants, whenever the critical service provider proposes to change its technology. Many critical service providers will not be able to comply with or operationalise this requirement, as such providers operate on a one-to-many basis with services and features that are frequently updated and improved and that any customer anywhere in the world can choose to use at any time. For example, a large cloud service provider will have millions of customers all over the world and will not be able to consult with individual operators or participants each time it plans to update its technology. Therefore, a requirement to consult with operators before updating technology might prevent cloud service providers from offering services to FMI operators in New Zealand, which would limit operators' ability to access the most appropriate information technology infrastructure and services for their needs.

Recommendation 4: AWS recommends that the RBNZ and FMA delete of "Proposed changes to a critical service provider's technology should include a comprehensive consultation with an operator and, where relevant, its participants" from Section 17B.14 of the Guidance. Instead, we recommend that the guidance state: "***An operator should require a critical service provider to regularly review its technology plans, including assessments of its technologies and the processes it uses for implementing change.***" We believe that this will address the intent of the guidance to ensure that operators are assured that their critical service providers have in place highly effective plans and mechanisms for managing changes in

their technologies and processes, without placing overly prescriptive or unreasonable transactional burdens on operators and their critical service providers, which may not achieve the underlying intention of the standard and guidance.

Communications to other participants (Clause 3 of 17B Standard, and Guidance 17B.16 and 17B.17)
AWS is concerned that Clause 3 of the 17B Standard and Section 17B.16 of the Guidance will create security risks and will require critical service providers to breach contractual and confidentiality obligations they owe to their customers. Clause 3 of the 17B Standard requires operators to disclose the FMI's dependencies on critical service providers to participants. This creates a security risk because details of the dependencies may be highly sensitive and, if obtained by a bad actor, may increase the risk of interference or cyber-attack. While participants would presumably be expected to keep the information confidential, AWS's experience is that increased dissemination of sensitive customer information across multiple organisations inherently increases the chances of inadvertent disclosure or interference. Further, Section 17B.16 of the Guidance requires a critical service provider to provide the FMI's participants (where they are affected) with sufficient information to clearly understand their roles and responsibilities. A critical service provider may not be in a position to identify and communicate directly with the FMI's participants (as it would only have a relationship and contract with the operator), and will typically owe contractual and confidentiality obligations to the operator that prohibit it from disclosing information to participants directly. Therefore, a critical service provider should only be expected to communicate directly with the operator and the regulator, and it should be the operator's responsibility to communicate with participants as necessary.

Section 17B.17 of the Guidance outlines that critical service providers should be expected to have mechanisms to consult with the FMI operator and the broader market on any technical changes to its operations that may affect its risk profile. As above, while it is appropriate for a critical service provider to communicate directly with the operator, a critical service provider should not be expected to communicate with the wider industry or to consult with operators before updating its technology.

Recommendations 5: AWS recommends that the RBNZ and FMA (a) delete "participants" from Clause 3 of the 17B Standard, or (b) provide guidance to clarify that operators only need to disclose high-level information about dependencies on critical service providers (e.g., "Operator A uses critical service provider B").

Recommendation 6: AWS recommends that the RBNZ and FMA delete all reference to FMI participants from Section 17B.16 of the Guidance.

Recommendation 7: AWS recommends that the RBNZ and FMA delete "As a part of its communication procedures and processes, a critical service provider should be expected to have mechanisms to consult with the FMI and the broader market on any technical changes to its operations that may affect its risk profile, including incidences of absent or non-performing risk controls of services" from Section 17B.17.

Notification to the regulator (Guidance 23B.13)
The Guidance requires an operator to notify the regulator within a maximum of two hours after the occurrence of an outage. While we understand the two-hour timeframe is intended to reflect the criticality of FMIs to the New Zealand financial system, two hours is an exceptionally tight timeframe that may not be possible in all circumstances. AWS is concerned that this Guidance may lead to operators insisting that third-party service providers undertake notification and response deadlines that are impossible to operationalise (and therefore impossible to accept) for some types of services, which may result in limiting the number of available service providers to FMIs and which may not be in a position to provider other important services and capabilities to the FMIs.

Recommendation 8: AWS recommends that the RBNZ and FMA delete the maximum timeframe of two hours from Section 23B.13 of the Guidance, and maintain a standard that the operator will update the regulator 'as soon as possible' once it has been notified of any potential or actual outage by a service provider. This allows for appropriate incident response, investigation and escalation by the service provider and the operator. AWS recommends that the RBNZ and FMA clarify that the reporting responsibility applies to the operator.

Service provider due diligence – reliance on recognised standards (Guidance on Standard 17B)

In the guidance on Standard 17B, it is unclear how an operator would verify that it has conducted satisfactory due diligence on critical service providers. To address this, AWS suggests that the RBNZ and the FMA permit operators to rely on industry-recognised certifications and standards. For example, AWS has achieved compliance with dozens of independent certifications, including System and Organization Controls Reports 1, 2 and 3, C5, PCI-DSS and ISO 27001, which encompass thousands of controls (see AWS Compliance Programs). Independent assurance reports and compliance programs are made available to customers at no expense through AWS Artifact.

Recommendation 9: AWS recommends that the RBNZ and the FMA explicitly identify that obtaining and reviewing up to date industry-recognised independent certifications and standards is a preferred method for operators to demonstrate that they have conducted satisfactory due diligence on critical service providers.

Inclusion of clear references to the New Zealand Information Security Manual (NZISM) and international best practice standards

In September 2022, the Government Communications Security Bureau (GCSB) released version 3.6 of the New Zealand Information Security Manual (NZISM).[2] This most recent update of the NZISM included for the first time a chapter providing clear guidance on the appropriate recommendations and controls for the use of public cloud services, such as AWS. In support of the New Zealand government's cloud first policy for RESTRICTED and below workloads, the new chapter (Chapter 23) provides guidance on the security concepts and architecture patterns for the use of public cloud services based on the widely accepted "Zero Trust" concepts and principles and the effective use of shared responsibility models. The NZISM now provides essential ("baseline") controls and additional good and recommended practice controls for the use of public cloud services, and guidance for effective risk management while using public cloud services. The NZISM is consistent with a wide variety of risk management, governance, assurance and technical standards, including the ISO/IEC 2700x series, as well as IETF, OASIS, NIST and other recognised standards bodies. Additionally, the Government Communications Security Bureau (GCSB) has undertaken a programme of work with industry to develop 'Baseline Security Templates'[3] mapped to the NZISM requirements. The baseline security templates support adoption of continuous assurance (certification) processes for cloud adoption in alignment with the "Zero Trust" model. As part of this collaboration, AWS has developed an NZISM Conformance Pack, NZISM operational best practices and an NZISM implementation guide for AWS, which allow organisations to map their AWS environments to NZISM baseline/essential controls.

Recommendation 10: AWS recommends that the FMI Guidance refer explicitly to the use of NZISM and related tools (such as NZISM baseline security templates) that relate to the use of technology services, including public cloud services. We believe it is useful for FMIs to understand that there is clear guidance available through the NZISM relating to the use of cloud services for some classified government

[2] https://www.nzism.gcsb.govt.nz/

[3] https://www.nzism.gcsb.govt.nz/home/introduction-to-the-nzism-baseline-security-templates/

workloads, and that detailed concepts and controls have been developed for the use of public cloud services. We further recommend inclusion of clear references to other widely recognised standards (such as NIST, ISO/IEC 2700x series) to support FMIs and operators in achieving information security and resilience best practices, and which can serve as effective frameworks for ensuring that their third party service providers are operating to well established standards for operational resilience, security and risk management.

Thank you once again for the opportunity to comment on the FMI Standards and Guidance. As noted above, we would be most grateful for an opportunity to engage with the authors in relations to several of the broad statements that are addressed in our submission above. We are of the view that an opportunity to present in greater detail the operating model and capabilities of a hyperscale public cloud provider, such as AWS, could provide important insights about cloud technology that would assist in the finalisaton of the Guidance.

Yours sincerely,

Paul Keating
Head of Public Policy, New Zealand
Amazon Web Services

APPENDIX A

ADDITIONAL ISSUES AND RECOMMENDATIONS RELATING TO THE

DRAFT FMI STANDARDS AND RECOMMENDATIONS

#	Reference	Issue	Recommendation
FMI Standards Exposure Drafts			
1.	**17A (Contingency Plans) – Clause 1(e)**	There is a risk that operators may perceive that the reasonable standard for recovery in *all* scenarios is two hours. While we understand the two-hour timeframe is intended to reflect the criticality of FMIs to the NZ financial system, two hours is an exceptionally tight timeframe that may not be possible in all circumstances.	AWS recommends that the RBNZ and FMA delete "and if recovery within 2 hours is not possible, the reasons why" from Clause 1(e) and the corresponding guidance in 17A.8. FMIs should be able to assess what timeframes are reasonable and achievable in each scenario.
2.	**17B (Critical Service Providers) – Clause 2(a)(i)**	The definition of "critical services" is very broad. As such, while all sophisticated critical service providers likely have policies and procedures in place for the continued availability of their services, there is a risk that this provision implies an expectation that critical service providers must provide 100% availability at all times and in all circumstances for any services that an operator designates as "critical services".	AWS recommends that the RBNZ and FMA clarify that "appropriate policies and procedures for the continued provision of critical services" will be dependent on the nature of the service and relationship between the parties, and will not require 100% availability service levels.
Financial Market Infrastructures Standards: Exposure Draft Guidance			
3.	**17A.5 (Contingency plans)**	Contingency planning is an area where we frequently encounter misunderstanding with customers, and where more prescriptive guidance would be valuable. Customers commonly conflate development of contingency plans to address short-term service provider issues (e.g. an unplanned technology outage which may be quickly resolved) with planning for longer term issues, such as a managed transition away from a provider that is failing to meet operational performance targets or long-term strategic objectives. This conflation of short-term issues with longer-term ones often causes customers to seek to develop unnecessarily complex, expensive and difficult-to-manage architectures, such as running the same workload in an active-active configuration across two different cloud service providers (i.e. "multi cloud" solution).	AWS recommends that the RBNZ and FMA revise Guidance 17A.5 to give specific examples of the types of scenarios that FMI operators should be planning and testing for, and the degree to which recovery capability should be validated, including ability to fail back to production (i.e. ability to return to the primary processing site or data center from the recovery site). The guidance should emphasise the difference between (a) short-term technical issues, which may be resolved by waiting for the provider to fix a problem, or the FMI operator enacting its own recovery plans, and (b) a longer term managed transition away from a provider who is no longer meeting requirements (which would take place over many weeks or months).
4.	**17B.11 (Reliability and resilience)**	This Section states that an operator should expect a critical service provider to: (a) record and report operational incidents; and (b) provide analysis on such incidents promptly in order to prevent recurrences that could have greater implications. As there is no defined term for "operational	AWS recommends that RBNZ and FMA (a) clarify what types of operational incidents should be reported, and (b) qualify this Section to ensure that critical service providers only need to report on operational incidents that are relevant to the operator and do not

#	Reference	Issue	Recommendation
		incident", this provision may lead to confusion of the severity and level of incidents that should be reported.	disclose any confidential or sensitive information relating to the critical service provider or any other customer.
5.	**17B.12 (Reliability and resilience)**	This Section outlines that a critical service provider's business continuity plans should include routine business continuity testing and a review of these test results to assess the risk of a major operational disruption. We consider that this paragraph, as worded, may lead FMI operators to seek copies of internal business continuity documents and management reporting which are commercially sensitive and may contain highly confidential internal network and system information which would present an extreme security risk if made externally available. A better approach would be to encourage review of independent assurance reports and industry-recognised certifications. This is the approach taken by the Bank of England/UK Prudential Regulation Authority in their Discussion Paper 22/3 on Operational Resilience: Critical third parties to the UK financial sector (p. 46, section 5.33)	AWS recommend that the RBNZ and FMA amend the Section as follows: "An operator should take reasonable steps to ensure that a critical service provider has robust business continuity and disaster recovery objectives and plans. **An operator should seek assurance that** these plans ~~should~~ include routine business continuity testing and **management** review of these test results to ~~assess the risk of a major operational disruption~~ **ensure appropriate resilience against a range of scenarios. Review of independent assurance reports and third-party certifications held by service providers is an efficient and effective way of achieving the required level of oversight."**
6.	**17C.57 (Management of third-party service providers)**	This Section states that it is common for third-party entities to have access to a company's data and its internal systems. While this may be true of some business process outsourcing (e.g. claims processing, credit decisioning) this is not true in all cases. For example, AWS customers maintain full control and ownership of their content. As such, AWS does not access or use customer content except in the limited circumstances outlined in our agreements with the customer.	AWS recommends that the RBNZ and FMA (a) delete the sentence below in its entirety, or (b) amend this sentence as follows: "**~~It is also common for these~~In some cases,** third-party entities may have access to have access to a company's data and its internal systems."
7.	**17C.66 (Contract terms)**	The list of cyber security considerations that the RBNZ and FMA suggested may be included in contracts will likely not be relevant to every third party service provider. This may cause confusion whenever operators seek to contract with third party service providers as they may expect specific provisions to be included in their agreements (even when not relevant to the of the services contemplated under the agreement).	AWS recommends that the RBNZ and FMA modify the Section as follows: "This may include, **where appropriate and relevant,** roles and responsibilities of each involved party regarding data access, incident response and communication, business continuity planning, termination, and data portability, etcetera.**"**
8.	**17C.67 (Contract terms)**	This Section suggests that an operator could agree to allow a third party service provider to further subcontract only when the subcontractors can fully meet the obligations existing between the FMI and their outsourcing service providers.	AWS recommends that the RBNZ and FMA delete "An operator could agree to allow a third-party to subcontract only when the subcontractors can fully meet the obligations existing between the FMI and their outsourcing service providers.". Alternatively, we ask the

#	Reference	Issue	Recommendation
		While is it appropriate for a third party to be responsible for its subcontractors, it is not appropriate for an operator to control or have veto or consent rights over what subcontractors are used by a service provider. Many service providers have established subcontracting channels that assist the service provider to provide services to all its customers.	RBNZ and FMA to clarify that a third party service provider does not need to seek the consent of an operator in order to use subcontractors, as long as the third party takes responsibility for the acts and omissions of its subcontractors.
9.	**17C.68 (Contract terms)**	This Section recommends that operators consider portability and interoperability of their data and applications and include provisions in outsourcing contracts to avoid vendor lock-in. This will not be relevant to all third party contracts, due to the different nature of services provided by each third-party.	AWS recommends that the RBNZ and FMA (a) deletes this Section, or (b) amends this Section as follows: "**When applicable depending on the nature of the services,** we recommend that operators consider portability and interoperability of their data and applications and include provisions in its outsourcing contracts to avoid vendor lock-in."
10.	**17C.69(d) (Ongoing cyber risk management)**	This Section recommends that an operator should integrate third parties that provide services for the FMI's essential services into the FMI's response plan. There is a risk that this will be misinterpreted by operators as requiring third parties to participate in their response plans. This may lead to operators asking third-parties to contractually commit to assisting them with their cyber security responses, which may be operationally impossible depending on the nature of the services provided.	AWS recommends that the RBNZ and FMA clarify that operators are entirely responsible for executing their own cyber risk plans and responses.
11.	**17C.71 (Ongoing cyber risk management)**	This Section recommends that operators conduct response and recovery testing with any third party service providers. This provision will not apply to all third parties.	AWS recommends that the RBNZ or FMA (a) deletes this Section, or (b) amends this Section as follows: "**When reasonable and appropriate depending on the nature of the services,** we recommend that operators conduct response and recovery testing with any third-party service providers and use the testing results to improve the FMI's response and recovery plans."
12.	**Guidance 23B.9 (Material incident)**	AWS assumes that the RBNZ and FMA are applying an intentionally broad set of circumstances and definitions of 'material incident'. However, this may create the risk of operators over-reporting to their regulators and missing genuinely important notifications. For example, 'a security threat' is an exceptionally broad definition, which may	AWS recommends that the RBNZ and FMA update the guidance with more clearly and narrowly defined scenarios or worked examples of when an operator would be expected to notify its regulators.

#	Reference	Issue	Recommendation
		encompass a range of plausible scenarios, from an operational failure to apply routine patches to a zero-day vulnerability (i.e. a vulnerability in a system or device that has been disclosed but is not yet patched) being disclosed and actively exploited.	